Claims

1. A method to authenticate a mobile station in a mobile network, **characterized** in that the mobile station is authenticated with user-to-user data exchange.

2. A method according to claim 1, **characterized** in that the data is exchanged during call setup.

3. A method according to claim 1, **characterized** in that the data is exchanged during a call.

4. A method according to claim 1, ~~2 or 3,~~ **characterized** in that also an encryption key is agreed between two mobile stations.

5. A method according to claim 4, **characterized** in that the mobile stations execute a mutual authentication and key agreement protocol based on public-key cryptography.

6. A method according to claim 5, **characterized** in that a second mobile station is authenticated by

a) a first mobile station constructing and sending to the second mobile station a first message, the second mobile station receiving the first message,

b) constructing and sending a second message to the first mobile station,

c) the first mobile station receiving the second message, checking the validity of the information in the second message, if the information is verified valid the first mobile station accepting to share a shared encryption key K with the second mobile station, the first mobile station constructing and sending a third message to the second mobile station,

d) the second mobile station receiving the third message and verifying the validity of the information, if the information is valid the second mobile station accepting the sharing of the shared encryption key K with the first mobile station.

7. A method according to claim 6, **characterized** in that

a) the second mobile station is authenticated by the first mobile station selecting a prime number p, a generator a of a multiplicative group of integers modulo p when $p \geq a \geq 2$ and a random secret x when $p-2 \geq x \geq 1$, constructing and sending to the second mobile station the first message containing

$$a, p, a^x \bmod p,$$

b) the second mobile station receiving the first message and afterwards generating a secret y when $p-2 \geq y \geq 1$ and computing a second shared key $K_2 = (a^x)^y \bmod p$, signing a concatenation of exponentials $\{a^y, a^x\}$ and encrypting a result $S_B\{a^y, a^x\}$ with the second shared key leading to $E_K(S_B\{a^y, a^x\})$, constructing and sending the second message to the first mobile station containing

$$a^y \bmod p, cert_B, E_K(S_B\{a^y, a^x\}),$$

certificate $cert_B$ in the second message containing a signature verification key of the second mobile station, the exact contents of the certificate being of at least the following minimum

$$cert_B = (B, p_B, a, p, S_T\{B, p_B, a, p\}),$$

p_B being a public signature verification key of the mobile station B and S_T a signature transformation of a trusted authority T whose public signature verification key is known in the first and second mobile stations,

c) the first mobile station receiving the second message and afterwards computing a first shared encryption key $(a^y)^x \bmod p = (a^x)^y \bmod p = K_1$, checking the validity of the certificate $cert_B$ the first mobile station, when the certificate $cert_B$ is valid the encrypted part $E_K(S_B\{a^y, a^x\})$ of the second message is decrypted to receive a signature $S_B\{a^y, a^x\}$ and the signature $S_B\{a^y, a^x\}$ is verified with a public signature verification key p_B of the second mobile station, if the signature $S_B\{a^y, a^x\}$ is verified valid the first mobile station accepts to share the shared encryption key K_1 with the second mobile station,

d) the first mobile station signing a concatenation of exponentials $\{a^x, a^y\}$ and encrypting result $S_A\{a^x, a^y\}$ with the first shared key K_1 leading to $E_K(S_A\{a^x, a^y\})$,

the first mobile station constructing and sending the third message to the second mobile station containing

$$cert_A, E_K(S_A\{a^x, a^y\}),$$

$cert_A$ including corresponding information with $cert_B$ of the first mobile station, exact contents of the certificate $cert_A$ being at least of the following minimum

$$cert_A = (B, p_A, a, p, S_T\{B, p_A, a, p\}),$$

p_A being a public signature verification key of the first subscriber and S_T a signature transformation of a trusted authority T whose public signature verification key is known by the first and second mobile stations,

e) the second mobile station receiving the third message and verifying validity of the $cert_A$, decrypting $E_A(S_A\{a^x, a^y\})$ and verifying validity of signature of $S_A\{a^x, a^y\}$, if all the signatures are valid the second mobile station accepting sharing of the second shared encryption key K_2 with the first mobile station.

8. A method according to ~~any preceding claim 1 to 7~~ claim 1, **characterized** in that the data is exchanged through user-to-user signalling.

9. A cellular communications system, where the first and second mobile stations are wireless connected with via base stations, **characterized** in that it comprises

a) a first mobile station, that constructs and sends a first message, receives and verifies the validity of a second message and when the information is verified valid accepts to share a shared encryption key K, constructs and sends a third message,

b) a second mobile station, that receives the first message and constructs and sends the second message, receives and verifies the validity of the third message and when the information is valid accepts to share the shared encryption key K with the first mobile station, and

c) at least one mobile switching centre.

10. A communications system according to claim 9, **characterized** in that it comprises two mobile switching centres connected together with ISDN.

11. A mobile station, **characterized** in that it comprises

a) a processor to perform operations needed to form and verify messages, to implement authentication and key agreement procedures,

b) a memory, where procedures and messages are stored with necessary parameters and variables,

c) output means, on which commencement of extra secure communication is presented to a user of the mobile station,

d) input means to enable validation of the extra secure communication,

e) a transmitter/receiver and an antenna to transform information to radio waves from digital signals and vice versa.

12. A mobile station according to claim 11, **characterized** in that the output means comprises a display.

13. A mobile station according to claim 11, **characterized** in that the input means comprises a keyboard.

14. A mobile station according to claim 11, **characterized** in that it is designed to GSM standards.

15. A mobile station according to claim 11, **characterized** in that it is designed to UMTS standards.